BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUTRY WILLIS, individually and on behalf of all others similarly situated, Plaintiff, v. INMARKET MEDIA, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Autry Willis ("Plaintiff") by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge, against Defendant InMarket Media, LLC. ("InMarket" or "Defendant").

NATURE OF THE ACTION

1. InMarket violates state law by first acquiring and tracking consumers' precise geolocation data and other data through the use of spyware called "InMarket SDK" and then profiting from that data by selling it to others. The data can include consumers' movements to and from sensitive locations, like locations associated with medical care, reproductive health, religious worship, mental health, rallies, demonstrations, or protests.

2. Plaintiff is an individual who asserts claims on behalf of herself and other similarly situated individuals for unjust enrichment and violations of California privacy statutes.

3. By selling this data without consent, Defendant has been unjustly enriched and has violated Plaintiff's privacy rights, state consumer protection and privacy statutes.

PARTIES

4. Plaintiff Autry Willis is a resident of Oakland, California. Plaintiff downloaded a third-party phone application which contained geolocation data tracking using Defendant's InMarket SDK (the "App"). At the time, Plaintiff believed that the App would not transfer Plaintiff's geolocation data to another entity for the purposes of selling said data. However, that was not the case: the App sent location data to Defendant when Plaintiff used the App. During that entire time, the App tracked the geolocation of Plaintiff. In turn, Defendant tracked Plaintiff's geolocation in California, and then sold that data for profit. Plaintiff suffered her primary injury in California. Plaintiff most recently used the App in or around December 2023.

5. During the time while Plaintiff used the App, Defendant took Plaintiff's geolocation data from the App and then sold Plaintiff's location data to other third parties.

6. Plaintiff has not consented to have her geolocation data sold to third parties for valuable consideration. If Plaintiff had been aware that Defendant would receive and sell her geolocation data to third parties, Plaintiff would have not used the App.

7. Defendant InMarket Media, LLC, is a Delaware limited liability corporation with its principal place of business in Austin, Texas.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the class is a citizen of a state different from any Defendant, the amount in controversy exceeds $5 million, exclusive of interest and costs, and the proposed class contains more than 100 members.

9. This Court has personal jurisdiction over Defendant because a substantial portion of the events giving rise to this cause of action occurred here. Plaintiff is domiciled and suffered her primary injury in this district.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

GENERAL BACKGROUND

A. InMarket Collects Sensitive Information From App Users On Over 300 Million Mobile Devices

11. InMarket is a digital marketing platform and data aggregator.

12. It collects consumer location data through its software development kit (the "InMarket SDK").

13. InMarket SDK is a collection of development tools that can be incorporated into a mobile application.

14. InMarket SDK's function is to collect the location data of all mobile application users which have InMarket SDK spyware embedded and transmit the consumer's precise location back to Defendant.

15. Thus, through the use of its spyware, InMarket monitors, tracks, and identifies consumers in real time, including Plaintiff and other putative class members.

16. Defendant incorporates InMarket SDK, into more than 300 third party apps, which have been downloaded onto over 390 million unique devices since 2017.

17. Apps that incorporate the InMarket SDK request access to the location data generated by a mobile device's operating system.

18. Critically, if the user allows access, the InMarket SDK receives the device's precise latitude and longitude, along with a timestamp and unique mobile device identifier, as often as the mobile device's operating system provides it— ranging from almost no collection when the device is idle, to every few seconds when the device is actively moving—and transmits it directly to Defendant's servers.

19. As a result, from 2016 to the present, about 100 million unique devices sent Defendant location data *each year*.

20. Defendant collects sensitive information from consumers, including where they live, where they work, where they worship, where their children go to school or obtain child care, where they received medical treatment (potentially revealing the existence of medical conditions), whether they went to rallies, demonstrations, or protests (potentially revealing their political affiliations), and any other information that can be gleaned from tracking a person's day-to-day movements.

21. This information is collected with several identifiers (including a unique mobile device identifier). Defendant has retained this information for up to five years.

B. Defendant Monetizes Users' Location Data Through Targeted Advertising

22. Defendant sorts consumers based on their visits to points of interest into audience segments to which it can target advertising.

23. Defendant has created or maintains almost two thousand distinct advertising audience segments.

24. For example, an InMarket brand client can target shoppers who are likely to be low-income millennials; well-off suburban moms; parents of preschoolers, high-school students, or kids who are home-schooled; Christian church goers; convenience-sensitive or price-sensitive; single parents or empty-nesters; affluent savers or blue collar workers; "healthy or wealthy" or "wealthy and not healthy," to name only a selection of the categories InMarket offers or has offered to its brand clients.

25. InMarket classifies audiences based on both past behavior and predictions it makes about consumers based on that behavior.

26. For example, if a consumer's past location data shows that she has visited a car dealership, InMarket can combine that information with the consumer's attributes purchased from other sources (age, income, family structure, education level), and can potentially predict that she may be in the market for a certain type of vehicle.

27. The InMarket SDK displays the ads and determines which ads appear in which apps incorporating the SDK.

28. Defendant additionally offers advertisers a product that sends push notifications based on a consumer's location and "geofencing," the creation of a virtual fence around a particular point of interest. When the InMarket SDK transmits a location that is inside a virtual fence, the app will send a push notification for a particular ad.

29. For example, a consumer who is within 200 meters of a pharmacy might see an ad for toothpaste, cold medicine, or some other product sold at that location.

30. Finally, Defendant also makes its advertising audience segments available on real-time bidding platforms. An advertiser using one of these platforms can select an advertising audience, and identify the amount that it is willing to pay (that is, its bid) each time its ad appears on a mobile device that is a part of that audience.

31. The advertiser's ad will appear on a particular device if it has the highest bid for that device.

32. Defendant receives some revenue each time an advertiser uses one of its audiences in this process.

C. Defendant Fails To Verify That Users Of Third-Party Apps Incorporating InMarket's SDK Have Been Notified That Their Location Data Will Be Used To Target Advertising

33. Defendant does little to verify that third-party apps incorporating its SDK obtain informed consumer consent before granting InMarket access to their sensitive location data.

34. InMarket additionally neither collects nor retains records of the disclosures that third-party apps incorporating the InMarket SDK provide consumers before accessing their location data.

35. In fact, InMarket does not require the third-party apps that incorporate its SDK to obtain informed consumer consent.

36. Even if these third-party app developers wanted to provide adequate disclosure to their users about InMarket's use of their location data, InMarket does not provide the developers with sufficient information to provide that notice.

37. Specifically, InMarket's contract with third-party app developers merely states that InMarket will serve ads on the developer's apps in return for developers passing user information to InMarket, including precise location and advertising identifiers.

38. Defendant does not disclose that information collected from these third-party users will be supplemented and cross-referenced with purchased data and analyzed to draw inferences about those users for marketing purposes.

39. Defendant therefore does not know whether users of hundreds of third-party apps that incorporate the InMarket SDK were informed of their data being collected and used for targeted advertising.

D. Defendant's Practices Cause and Are Likely to Cause Substantial Injury to Consumers

40. Because Defendant readily combined the location data of those users into its databases and systems without confirming user consent, Defendant obtained and used that data without informed user consent, resulting in consumer injury.

41. In addition, after collecting sensitive precise location data about consumers' daily movements, Defendant retains that information longer than reasonably necessary to accomplish the purpose for which that information was collected and thereby exposes consumers to significant unnecessary risk. Specifically, InMarket has retained consumer location data for five years prior to deletion.

42. This unreasonably long retention period—significantly increases the risk that this sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing sensitive information about that consumer's life.

43. Defendant's comprehensive collection and long-term retention of location data subjects consumers to a likelihood of substantial injury through the exposure of their re-identified location.

FTC'S JANAURY 2023 COMPLAINT AGAINST DEFENDANT

44. In January 2023, the FTC took action against Defendant for allegations that are substantially identical to this complaint.

45. According to the FTC's complaint, Defendant's acts as described above constitutes a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

46. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

CLASS ALLEGATIONS

47. ***Class Definition.*** Plaintiff brings this action on behalf of a class of similarly situated individuals, defined as all persons in the United States whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "Class").

(a) ***California Subclass.*** Plaintiff also seeks to represent a subclass defined as all Class members who reside in California whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "California Subclass").

48. Excluded from the Class and Subclass are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, and members of the judge's staff, and the judge's immediate family.

49. Subject to additional information obtained through discovery, the foregoing class definitions may be modified or narrowed by an amended complaint, or at class certification, including through the use of multi-state subclasses to account for material differences in state law, if any.

50. Members of the Class and California Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and California Subclass number in the millions. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

51. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include but are not limited to whether Defendant's sale of geolocation data without consent constitutes unjust enrichment.

52. The claims of the named Plaintiff are typical of the claims of the Class in that the named Plaintiff's data was sold by Defendant without her consent, and the named Plaintiff suffered injury as a result of Defendant's conduct.

53. Plaintiff is an adequate representative of the Class and California Subclass because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

54. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability

issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Invasion of Privacy

55. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

56. Plaintiff brings this claim individually and on behalf of the California Subclass.

57. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

58. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

59. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. … It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. And Amends. To Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting).

60. Plaintiff and the California Subclass members have a legally protected privacy interest, as recognized by the California Constitution, CIPA, common law and the 4th Amendment to the United States Constitution.

61. Plaintiff and California Subclass members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiff and California Subclass members were not aware and could not have reasonably expected that unknown third party would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiff's and California Subclass members' sensitive information with other parties.

62. Defendant's conduct violates, at a minimum:

(a) The right to privacy in data, communications and personal information contained on personal devices;

(b) The California Constitution, Article I, Section 1;

(c) The California Wiretapping Act;

(d) The California Invasion of Privacy Act; and

(e) The California Computer Data Access and Fraud Act.

63. Defendant's conduct in secretly intercepting and collecting Plaintiff's and California Subclass members' personal information, location data, and communications is an egregious breach of social norms and is highly offensive to a reasonable person.

64. Defendant's conduct in analyzing, using, and sharing with third parties the personal information and communications that Defendant intercepted and took from Plaintiff's and California Subclass members is an egregious breach of societal norms and is highly offensive to a reasonable person, and violates Plaintiff's and California Subclass members' reasonable expectations of privacy.

65. Plaintiff and California Subclass members did not consent for Defendant to track, collect, or use their personal information and communications.

66. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiff and California Subclass members were injured and suffered damages. Plaintiff and California Subclass members are entitled to equitable relief and just compensation in an amount to be determined at trial.

67. Defendant was unjustly enriched as a result of its invasion of Plaintiff's and California Subclass members' privacy.

COUNT II
Violation of the California Computer Data Access and Fraud Act
Cal. Penal Code. § 502

68. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

69. Plaintiff brings this claim individually and on behalf of the California Subclass.

70. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals … from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code §502(a). The enactment of CDAFA was motivated by the finding that "the proliferation of computer technology has resulted in a concomitant proliferation of … unauthorized access to computers, computer systems, and computer data." *Id.*

71. Plaintiff's and California Subclass members' smartphone constitute "computers" within the scope of the CDAFA.

72. Defendant violated the following sections of the CDAFA:

(a) Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission … use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

(b) section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

(c) Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

73. Defendant knowingly accessed Plaintiff's and California Subclass members' smartphones without their permission by including within the SDK, that Defendant provides to developers, software that intercepts and transmits data, communications, and personal information concerning Plaintiff and California Subclass members.

74. Defendant used data, communications, and personal information that it intercepted and took from Plaintiff's and California Subclass members' smart phones to wrongfully and unjustly enrich itself at the expense of Plaintiff and California Subclass members.

75. Defendant took, copied, intercepted, and made use of data, communications, and personal information from Plaintiff's and California Subclass members' smartphones.

76. Defendant knowingly and without Plaintiff's and California Subclass members' permission accessed or caused to be their smartphones by installing without Plaintiff's and California Subclass members' informed consent software that intercepts and/or takes data, communications, and personal information concerning Plaintiff and California Subclass members.

77. Plaintiff and California Subclass members are residents of California, and used their smartphones in California. Defendant accessed or caused to be accessed Plaintiff's and California Subclass members' data, communications, and personal information from California. On information and belief, Defendant uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning Plaintiff and California Subclass Members.

78. Defendant was unjustly enriched by intercepting, acquiring, taking, or using Plaintiff's and California Subclass members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

79. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiff and California Subclass Members suffered damages.

80. Pursuant to CDAFA Section 502(e)(1), Plaintiff and California Subclass Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

81. Pursuant to CDAFA Section 502(e)(2), Plaintiff and California Subclass Members seek an award of reasonable attorney's fees and costs.

82. Pursuant to CDAFA Section 502(e)(4), Plaintiff and California Subclass Members seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.

COUNT III
Use of a Pen Register or Trap and Trace Device
Cal. Penal Code § 638.51

83. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

84. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

85. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

86. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

87. Defendant's SDK constitutes a "pen register" because it is a device or process that records addressing or signaling information—Plaintiff's and California Subclass Members' location data and personal information—from the electronic communications transmitted by their smartphones.

88. Defendant was not authorized by any court order to use a pen register to track Plaintiff's and California Subclass members' location data and personal information.

89. As a direct and proximate result of Defendant's conduct, Plaintiff and California Subclass Members suffered losses and were damages in an amount to be determined at trial.

COUNT IV
Violation of the California Wiretapping Act
Cal. Penal Code § 631

90. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

91. Plaintiff brings this claim individually and on behalf of the California Subclass.

92. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

93. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

94. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.*

95. The California Wiretapping Act prohibits:

> "any person [from using] any machine, instrument, [] contrivance, or in any other manner … [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

96. Plaintiff's and California Subclass Members' specific user input events and choices on their mobile devices that are tracked by Defendant's SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the Wiretapping Act.

97. Plaintiff and California Subclass Members are residents of California, and used their smartphones within California. As such, Defendant intercepts, reads, or attempts to read Plaintiff's and Class members' data, communications, and personal information in California.

98. On information and belief, Defendant uses servers in California to intercept, track, process, or otherwise use Plaintiff's and California Subclass members' data, communications, and personal information within California.

99. Defendant intercepts Plaintiff's and California Subclass Members' communications while they are in transit to and from Plaintiff's and California Subclass Members' smartphones and the apps, app developers, and cellphone towers; Defendant transmits a copy of Plaintiff's and California Subclass Members' communications to itself. Defendant uses the contents of the communications to sell to third parties and in other methods for its own pecuniary gain.

100. Neither Defendant nor any other person informed Plaintiff and California Subclass members that Defendant was intercepting and transmitting Plaintiff's private communications. Plaintiff and California Subclass Members did not know Defendant was intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendant and thereafter transmitted to others.

101. Defendant's SDK constitutes a machine, instrument, contrivance or other manner to track and intercept Plaintiff's and California Subclass members' communications while they are using their smartphones.

102. Defendant uses and attempts to use or communicate the meaning of Plaintiff's and California Subclass members' communications by ascertaining their personal information, including their geolocation and places that they have visited, in order to sell Plaintiff's and California Subclass members' personal information to third parties.

103. At all relevant times to this complaint, Defendant intercepted and recorded components of Plaintiff's and the putative California Subclass' private telephone communications and transmissions when Plaintiff and other California Subclass Members accessed Defendant's software via their cellular mobile access devices within the State of California.

104. At all relevant times to this complaint, Plaintiff and other California Subclass Members did not know Defendant was engaging in such interception and recording and therefore could not provide consent to have any part of their private and confidential video conferencing communications intercepted and recorded by Defendant and thereafter transmitted to others.

105. At the inception of Defendant's illegally intercepted and stored her geolocation and other personal data, Defendant never advised Plaintiff or the other California Subclass Members that any part of this sensitive personal data would be intercepted, recorded and transmitted to third parties.

106. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email.

107. Defendant's use of its SDK is both a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

108. At all relevant times, by using Defendant's SDK as well as tracking Plaintiff's and California Subclass Members' geolocation, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff and California Subclass Members on the one hand, and the specific sites and locations Plaintiff and California Subclass Members visited on the other.

109. At all relevant times, by using Defendant's geolocation tracking software technology, Defendant willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative California Subclass members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

110. Plaintiff and California Subclass Members did not consent to any of Defendant's actions in implementing these wiretaps within its geolocation tracking software. Nor have Plaintiff or California Subclass Members consented to Defendant's intentional access, interception, reading, learning, recording, and collection of Plaintiff and California Subclass Members' electronic communications.

111. Plaintiff's and the California Subclass Members' devices of which Defendant accessed through its unauthorized actions included their computers, smart phones, and tables and/or other electronic computing devices.

112. Defendant violated Cal. Penal Code § 631 by knowingly accessing and without permission accessing Plaintiff and California Subclass Members' devices in order to obtain their personal information, including their device and location data and personal communications with others, and in order for Defendant to share that data with third parties, in violation of Plaintiff's and California Subclass Members' reasonable expectations of privacy in their devices and data.

113. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiff's and the California Subclass Members' personally identifiable information and personal communications with others.

114. As a direct and proximate result of Defendant's violation of the Wiretapping Act, Plaintiff and California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

115. Defendant was unjustly enriched by its violation of the Wiretapping Act.

116. Pursuant to California Penal Code Section 637.2, Plaintiff and California Subclass members have been injured by Defendant's violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT V
Unfair Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

117. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

118. Plaintiff brings this claim individually and on behalf of the California Subclass.

119. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, which prohibits, *inter alia*, "any unlawful, *unfair*, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200 (emphasis added).

120. Defendant engaged in business acts and practices which are "unfair" under the UCL, including surreptitiously collecting, tracking, using and disseminating Plaintiff's and California Subclass Members' personal information, geolocation data, and communications.

121. Defendant also engaged in a number of practices designed to perpetuate the scheme and the stream of revenue it generates. Those practices, which are unfair separately and particularly when taken together, include but are not limited to invasion of Plaintiff's and California Subclass members' privacy; surreptitiously tracking Plaintiff's and California Subclass members' location; surreptitiously accessing Plaintiff's and California Subclass members' cellphones without authorization; surreptitiously obtaining personal data from Plaintiff's and California Subclass

members' cellphones; surreptitiously intercepting and recording Plaintiff's and California Subclass members' communications.

122. Unfair acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers themselves could not reasonably have avoided. Defendant's conduct alleged is unfair under all of these tests.

123. As a direct and proximate result of Defendant's unfair practices, Plaintiff and California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

124. Plaintiff seeks to enjoin further unfair acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Profession Code §17200.

COUNT VI
Unlawful Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

125. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

126. Plaintiff brings this claim individually and on behalf of the California Subclass.

127. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, which prohibits, *inter alia*, "any *unlawful*, unfair, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code §17200 (emphasis added).

128. In the course of their business, Defendant repeatedly and regularly engaged in unlawful acts or practices that imposed a serious harm on consumers, including Plaintiff and California Subclass members.

129. Defendant's acts and practices are unlawful because Defendant violated, and continues to violate:

(a) The Constitution of California, Article I, Section 1;

(b) The California Computer Data Access and Fraud Act;

(c) The California Invasion of Privacy Act; and

(d) Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45.

130. As a direct and proximate result of Defendant's unlawful practices, Plaintiff and California Subclass members were injured and suffered damages, a loss of privacy, and loss of value of their personal information in an amount to be determined at trial.

131. Plaintiff seeks to enjoin further unlawful acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Professions Code §17200.

COUNT VII
Unjust Enrichment or Restitution

132. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

133. Plaintiff brings this claim individually and on behalf of the Class.

134. Plaintiff and members of the Class conferred a benefit on Defendant through the use and dissemination of Plaintiff's and Class members' personal information, geolocation data, and communications.

135. Defendant received and is in possession of Plaintiff's and Class members' personal information, geolocation data, and communications, which Defendant used and disseminated for its own monetary benefit.

136. It is unjust under the circumstances for Defendant to retain the benefit conferred by Plaintiff and Class members without compensating them.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class under Fed. R. Civ. P. 23 and naming Plaintiff as representatives of the Class and the California Subclass and Plaintiff's attorneys as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff, the Class, and the California Subclass on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For an order awarding Plaintiff and the Class and California Subclass their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: January 26, 2024

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff